

Haavoittuvuuksien ilmoittamiskäytäntö

Tietoturva haavoittuvuuksien vastuullinen ilmoittaminen, tutkiminen ja korjaaminen

Versio	Voimaantulo päivä	Asiakirjan omistaja	Yhteystiedot
1.0	Syyskuu 2026	SALUS Controls PLC:n tietoturvatiimi	security@saluscontrols.com

1. Johdanto.....	2
2. Soveltamisala.....	2
3. Haavoittuvuuden ilmoittaminen.....	2
4. Ilmoitukseen sisällytettävät tiedot.....	3
5. Käsittelyprosessi.....	3
6. Riskiperusteinen korjaaminen.....	4
7. Koordinoitu haavoittuvuuden julkistaminen.....	4
8. Tietoturvapäivitysten tuki.....	4
9. Soveltamisalan ulkopuolella.....	5
10. Vastuullinen tietoturvatutkimus.....	5
11. Yhteystiedot.....	5
12. Käytännön päivitykset.....	6
13. Tunnustus.....	6

1. Johdanto

SALUS Controls PLC on sitoutunut suojaamaan tuotteidensa, palveluidensa ja asiakkaidensa tietoturvaa. Toivotamme tervetulleiksi vastuulliset ilmoitukset asiakkailta, tietoturvatutkijoilta, kumppaneilta, kehittäjiltä ja muilta tietoturvayhteisön jäseniltä, jotka havaitsevat SALUS Controls PLC:n tuotteisiin tai palveluihin mahdollisesti vaikuttavia tietoturva-avaavuuksia.

Tavoitteemme on tutkia mahdolliset haavoittuvuusilmoitukset nopeasti, viestiä ilmoittajan kanssa asianmukaisesti koko prosessin ajan ja toteuttaa käyttäjien suojaamiseksi oikeasuhtaiset korjaus- tai lieventämistoimet.

Ilmoita mahdollisista tietoturva-avaavuuksista luottamuksellisesti osoitteeseen security@saluscontrols.com. SALUS Controls PLC vahvistaa vastaanoton kolmen arkipäivän kuluessa ja kaikissa tapauksissa viimeistään seitsemän kalenteripäivän kuluessa. Tämä vahvistus ainoastaan vahvistaa tietojen vastaanoton eikä tarkoita, että ilmoitettu ongelma olisi todettu haavoittuvuudeksi.



2. Soveltamisala

Tätä käytäntöä sovelletaan tietoturva-avaavuuksiin, jotka vaikuttavat seuraaviin:

- SALUS Controls PLC:n tuotteet
- Laitteohjelmistot ja ohjelmistot
- Mobiilisovellukset
- Pilvipalvelut
- Julkisesti käytettävissä olevat verkkosovellukset ja verkkosivustot

Tuotteiden asennusta, määrittystä, takuuta tai muita kuin tietoturva-asioita koskevissa kysymyksissä ota yhteyttä asiakastukeemme tavallisten tukikanavien kautta.

Hyväksymme SALUS-tuotteita koskevat tietoturvailmoitukset tuotteen elinkaaren vaiheesta riippumatta. Julkaistun tietoturvatuen piirissä olevien tuotteiden haavoittuvuudet ja tietoturvapäivitykset käsitellään sovellettavien lakisääteisten velvoitteiden mukaisesti. Tukikauden ulkopuolella olevista tuotteista SALUS Controls PLC arvioi silti ilmoitukset ja voi riskin, teknisen toteutettavuuden ja sovellettavien velvoitteiden perusteella tarjota lieventämistoimia, siirtymisohjeita tai muuta ohjeistusta.

3. Haavoittuvuuden ilmoittaminen

Jos uskot havainneesi tietoturva haavoittuvuuden, ilmoita siitä luottamuksellisesti sähköpostitse osoitteeseen security@saluscontrols.com.

Ilmoituksen voi tehdä nimettömänä. Nimen tai kaksisuuntaisen yhteydenpitotavan puuttuminen ei estä ilmoituksen vastaanottoa tai alustavaa arviointia, mutta se voi rajoittaa mahdollisuuksiamme pyytää lisätietoja, antaa tilannepäivityksiä tai tarjota julkista tunnustusta.

Hyväksymme alkuperäisen ilmoituksen tavallisella sähköpostilla tai muulla kanavalla. Jos on tarpeen vaihtaa hyväksikäyttökoodia, tunnistetietoja, henkilötietoja, asiakasmäärittelyksiä tai muita arkaluonteisia tietoja, SALUS Controls PLC tarjoaa käytettävissä olevan turvallisen tavan viestinnän jatkamiseen. Ilmoittajan kyvyttömyys tai päätös olla käyttämättä salausta ei yksinään johda ilmoituksen hylkäämiseen.

4. Ilmoitukseen sisällytettävät tiedot

Jotta voimme tutkia ilmoituksesi tehokkaasti, sisällytä mahdollisuuksien mukaan seuraavat tiedot:

- Tuotteen nimi ja malli
- Laiteohjelmiston tai ohjelmiston versio
- Haavoittuvuuden kuvaus
- Ongelman toistamiseen tarvittavat vaiheet
- Odotettu ja toteutunut toiminta
- Mahdollinen tietoturva vaikutus
- Kuvakaappaukset, loikit tai konseptitodiste, jos saatavilla
- Halutut yhteystiedot jatkoyhteydenpitoa varten

Vältä arkaluonteisten henkilötietojen sisällyttämistä, elleivät ne ole tarpeen haavoittuvuuden osoittamiseksi.

Ilmoita myös, jos tiedossa, onko ongelma julkinen, hyödynnetäänkö sitä aktiivisesti, onko se vaikuttanut käyttäjiin tai onko se ilmoitettu toiselle toimittajalle, valmistajalle tai koordinaattorille. Kaikkia pyydettyjä tietoja ei tarvitse toimittaa, jotta voimme hyväksyä ja rekisteröidä ilmoituksen.

Koordinoidun julkistamisen aikana pääsy ei-julkisiin haavoittuvuustietoihin rajataan vain niitä tarvitseville. SALUS Controls PLC voi jakaa tarpeellisia tietoja tuotetiimeille, toimittajille, koordinaattoreille, asianomaisille osapuolille tai toimivaltaisille viranomaisille validointia, korjaamista, käyttäjien suojaamista ja lakisääteisten velvoitteiden noudattamista varten asianmukaisin luottamuksellisuus- ja tietosuojatoimin.

Haavoittuvuusilmoituksen yhteydessä toimitetut henkilötiedot käsitellään sovellettavan SALUS Controls PLC:n tietosuojaselosteen mukaisesti. Katso tietosuojaseloste:

<https://saluscontrols.com/fi/tietosuoja-evasteet/>.

5. Käsittelyprosessi

Saatuun ilmoituksesi SALUS Controls PLC:

- Vahvistaa vastaanoton kolmen arkipäivän kuluessa ja kaikissa tapauksissa viimeistään seitsemän kalenteripäivän kuluessa; mahdollisuuksien mukaan mukana on yksilöllinen tapaustunnus ja alustavat tilannetiedot.
- Tekee alustavan arvioinnin seitsemän työpäivän kuluessa
- Vahvistaa ilmoitetun haavoittuvuuden
- Arvioi sen vakavuuden ja mahdolliset vaikutukset
- Laatii tarvittaessa korjaussuunnitelman tai tietoturvapäivityksen
- Pitää sinut ajan tasalla tutkimus- ja korjausprosessin aikana
- Antaa aktiivisen tapauksen aikana olennaisen tilanpäivityksen vähintään 30 kalenteripäivän välein ja viestii aiemmin, jos vahvistettu laajuus, riski, korjaustapa tai julkistamispäivä muuttuu olennaisesti.
- Jos lisätietoja tarvitaan, voimme ottaa sinuun yhteyttä tutkimuksen aikana.

6. Riskiperusteinen korjaaminen

Vahvistetut haavoittuvuudet priorisoidaan teknisen vakavuuden, hyödynnettävyyden, vaikutuksen alaisten tuotteiden, mahdollisten vaikutusten, käyttäjäaltistuksen, aktiivisen hyväksikäytön todisteiden, saatavilla olevien lieventämistoimien ja turvallisen käyttöönoton tarpeiden perusteella. Numeerista pistemäärää voidaan käyttää arvioinnin tukena, mutta se ei yksin määrää korjausprioriteettia.

SALUS Controls PLC asettaa tapauskohtaisen korjaustavoitteen ja ilmoittaa olennaisista muutoksista ilmoittajalle. Jos välitön korjaus ei ole mahdollinen, ennen pysyvää korjausta voidaan antaa asianmukaisia lieventämis- tai riskin pienentämisohjeita.

7. Koordinoitu haavoittuvuuden julkistaminen

SALUS Controls PLC sopii ilmoittajan ja tarvittaessa toimittajien, koordinaattorien sekä muiden asianomaisten osapuolten kanssa tapauskohtaisen julkistamispäivän. Ajankohtaa voidaan muuttaa vakavuuden, aktiivisen hyväksikäytön, käyttäjäriskin, korjauksen ja käyttöönoton edistymisen, toimitusketjuriippuvuuksien sekä sovellettavien laki- tai viranomaisvelvoitteiden perusteella. Tavoitepäivän olennaisista muutoksista ilmoitetaan asianomaisille osapuolille.

SALUS Controls PLC voi nopeuttaa käyttäjille tiedottamista tai julkista julkistamista, jos haavoittuvuus on jo julkinen, sitä hyödynnetään aktiivisesti, se aiheuttaa kiireellisen käyttäjäriskin, sen vuotaminen on todennäköistä tai laki edellyttää ilmoittamista. Jos täydellistä korjausta ei vielä ole, SALUS voi antaa tilapäisiä lieventämis- tai riskin pienentämisohjeita helpottamatta tarpeettomasti hyväksikäyttöä.

Korjatuista haavoittuvuuksista julkaistaan helposti saatavilla olevia, ihmisen luettavissa olevia tietoturvatiedotteita. Tiedotteissa yksilöidään haavoittuvuus ja vaikutuksen alaiset tuotteet, julkaisu- ja tarkistuspäivät, mahdollinen vaikutus ja vakavuus, saatavilla olevat korjaus- tai lieventämistoimet, käyttäjiltä vaadittavat toimet ja yhteystiedot. Kolmansien osapuolten komponentteja koskeissa tiedotteissa voidaan viitata luotettaviin alkuperäislähteisiin, jos niiden avulla käyttäjät voivat selvittää, vaikuttaako asia SALUS-tuotteisiin.

Haavoittuvuustiedot asetetaan saataville myös yleisesti tunnistetussa koneellisesti luettavassa muodossa, ellei poikkeamiselle ole dokumentoitua ja hyväksyttyä perustetta. Julkaisua voidaan viivästyttää tai se voidaan jättää tekemättä vain, jos sovellettavat ehdot on arvioitu, dokumentoitu ja hyväksytty.

Kun sovellettava laki sitä edellyttää tai käyttäjien suojaaminen sitä vaatii, SALUS Controls PLC tiedottaa asianomaisille käyttäjille ja antaa saatavilla olevat lieventämis- tai korjausohjeet asianmukaisten, helposti käytettävien kanavien kautta.

8. Tietoturvapäivitysten tuki

SALUS Controls PLC tarjoaa tietoturvapäivityksiä kullekin soveltuvalle tuotteelle määritetyn tukikauden ajan. Tukikausi määritetään sovellettavien lakisääteisten vaatimusten mukaisesti ottaen huomioon tuotteen odotettu käyttöaika, luonne ja käyttäjien kohtuulliset odotukset.

Tukikausi on vähintään viisi vuotta, ellei tuotteen kohtuudella odoteta olevan käytössä lyhyempää aikaa, ja se voi olla pidempi, jos tuotteen odotettu käyttöikä sitä perustelee. Sovellettavan tukikauden päättymispäivä ilmoitetaan tuotetta koskevissa tiedoissa.

9. Soveltamisalan ulkopuolella

Kaikki mahdolliset tietoturvailmoitukset rekisteröidään ja arvioidaan alustavasti. Puhtaasti toiminnalliset, kaupalliset tai tukipalveluihin liittyvät asiat voidaan ohjata asianmukaiseen tukikanavaan. Jos ongelmaa ei aluksi voida toistaa, SALUS Controls PLC voi pyytää lisätietoja ja arvioida ilmoituksen uudelleen uuden näytön perusteella.

Teoreettisia ongelmia, fyysiseen pääsyyn liittyviä tilanteita, palvelunestotilanteita, sosiaalisen manipuloinnin skenaarioita ja kolmansien osapuolten riippuvuuksia arvioidaan niiden realistisen tietoturva vaikutuksen, hyödynnettävyyden sekä tuotteen tarkoitetun ja kohtuudella ennakoitavan käytön perusteella.

SALUS-tuotteeseen integroitujen, sen mukana toimitettujen tai sen käyttämien kolmannen osapuolen komponenttien haavoittuvuudet arvioidaan edelleen niiden SALUS-tuotteeseen kohdistuvan vaikutuksen perusteella.

10. Vastuullinen tietoturvatutkimus

SALUS Controls PLC tukee vilpittömässä mielessä tehtävää vastuullista tietoturvatutkimusta. Pyydämme tutkijoita:

- Toimimaan vastuullisesti ja eettisesti
- Välttämään tuotteiden, palveluiden tai asiakkaiden toiminnan häiritsemistä
- Välttämään asiakastietojen käyttöä, muuttamista tai poistamista
- Ilmoittamaan haavoittuvuudet luottamuksellisesti tässä käytännössä kuvatun prosessin mukaisesti
- Antamaan SALUS Controls PLC:lle kohtuullisesti aikaa tutkia ja korjata ongelma ennen julkista julkistamista
- Noudattamaan tietoturvatutkimuksessa kaikkia sovellettavia lakeja ja määräyksiä

Kun ilmoittaja toimii vilpittömässä mielessä, noudattaa tätä käytäntöä, välttää vahingon aiheuttamista ja ilmoittaa nopeasti, SALUS Controls PLC ei aio ryhtyä oikeustoimiin pelkästään tämän käytännön mukaisesti tehdyn tietoturvatutkimuksen vuoksi. Tämä lausuma ei oikeuta pääsyä kolmansien osapuolten järjestelmiin tai tietoihin, sido kolmatta osapuolta tai viranomaista eikä poista ilmoittajan velvollisuutta noudattaa sovellettavaa lakia ja hankkia tarvittavat luvat.

11. Yhteystiedot

Kaikissa tietoturvaan liittyvissä ilmoituksissa tai tätä käytäntöä koskevissa kysymyksissä ota yhteyttä:

SALUS Controls PLC:n tietoturvatiimi

Sähköposti: security@saluscontrols.com

12. Käytännön päivitykset

Tämä käytäntö tarkistetaan vähintään vuosittain sekä sovellettavien lakivaatimusten, ilmoituskanavien, tuotealueen tai haavoittuvuuksien käsittelyprosessien olennaisten muutosten jälkeen. Nykyinen versio, julkaisupäivä, viimeisin päivityspäivä ja käytännön omistaja näytetään julkaistun käytännön yhteydessä.

13. Tunnustus

Ilmoittajan suostumuksella SALUS Controls PLC voi mainita ilmoittajan nimen, nimimerkin tai organisaation joka tekee pätevän haavoittuvuusilmoituksen ja tukee koordinoitua julkistamista. Ilmoituksen voi tehdä nimettömästi, eikä tunnustuksesta kieltäytyminen vaikuta hyväksymiseen, priorisointiin tai korjauspäätöksiin.

Tämä käytäntö ei perusta haavoittuvuuspalkkio-ohjelmaa eikä takaa rahallisia tai muita palkkioita.